Upgrade Guide for FortiOS 3.0

www.fortinet.com

Upgrade Guide for FortiOS 3.0
24 April 2006
01-30000-0317-20060424

Trademarks

Regulatory compliance

FCC Class A Part 15 CSA/CUS

Contents

Introduction

Over the past year, Fortinet has been developing, testing and refining a new operating system for your FortiGate unit. FortiOS 3.0 is a more dynamic and robust operating system, offering you even better protection, blocking and monitoring features for your network.

The Upgrade Guide provides you with information on FortiOS 3.0, and addresses any issues that may arise concerning your current configuration. With these new features, and improvements to existing features, you need to know how they may or may not affect your current configuration.The guide provides you with information on backing up your current configuration, and installing FortiOS 3.0, on your FortiGate unit.

About this document

This document contains the following chapters:

- Upgrade Notes – Provides information on changes and new features for FortiOS 3.0.
- New features and changes – Provides information on what has changed from FortiOS v2.80MR11.
- Upgrading to FortiOS 3.0 – Describes how to install FortiOS 3.0, including addressing issues about FortiOS 3.0, backing up your current configuration settings, re-establishing connections after the upgrade, and verifying the upgrade installed successfully.
- Reverting to FortiOS v2.80MR11 – Describes how to downgrade your FortiGate unit to FortiOS v2.80MR11 and includes how to restore your configuration settings for FortiOS v2.80MR11.

Document conventions

The following document conventions are used in this guide:

- In the examples, private IP addresses are used for both private and public IP addresses.
- Notes and Cautions are used to provide important information:

Note: Highlights useful additional information.

Caution: Warns you about commands or procedures that could have unexpected or undesirable results including loss of data or damage to equipment.

Typographic conventions

FortiGate documentation uses the following typographical conventions:

Convention	Example
Keyboard input	In the Gateway Name field, type a name for the remote VPN peer or client (for example, `Central_Office_1`).

Code examples	`config sys global`
	`set ips-open enable`
	`end`

CLI command syntax	`config firewall policy`
	`edit id_integer`
	`set http_retry_count <retry_integer>`
	`set natip <address_ipv4mask>`
	`end`

Document names	*FortiGate Administration Guide*
Menu commands	Go to **VPN > IPSEC > Phase 1** and select Create New.
Program output	`Welcome!`
Variables	`<address_ipv4>`

Fortinet documentation

The most up-to-date publications and previous releases of Fortinet product documentation are available from the Fortinet Technical Documentation web site at http://docs.forticare.com.

The following FortiGate product documentation is available:

- *FortiGate QuickStart Guide*

  Provides basic information about connecting and installing a FortiGate unit.
- *FortiGate Installation Guide*

  Describes how to install a FortiGate unit. Includes a hardware reference, default configuration information, installation procedures, connection procedures, and basic configuration procedures. Choose the guide for your product model number.
- *FortiGate Administration Guide*

  Provides basic information about how to configure a FortiGate unit, including how to define FortiGate protection profiles and firewall policies; how to apply intrusion prevention, antivirus protection, web content filtering, and spam filtering; and how to configure a VPN.
- *FortiGate online help*

  Provides a context-sensitive and searchable version of the *Administration Guide* in HTML format. You can access online help from the web-based manager as you work.
- *FortiGate CLI Reference*

  Describes how to use the FortiGate CLI and contains a reference to all FortiGate CLI commands.

- *FortiGate Log Message Reference*

  Available exclusively from the Fortinet Knowledge Center, the FortiGate Log Message Reference describes the structure of FortiGate log messages and provides information about the log messages that are generated by FortiGate units.
- *FortiGate High Availability User Guide*

  Contains in-depth information about the FortiGate high availability feature and the FortiGate clustering protocol.
- *FortiGate IPS User Guide*

  Describes how to configure the FortiGate Intrusion Prevention System settings and how the FortiGate IPS deals with some common attacks.
- *FortiGate IPSec VPN User Guide*

  Provides step-by-step instructions for configuring IPSec VPNs using the web-based manager.
- *FortiGate SSL VPN User Guide*

  Compares FortiGate IPSec VPN and FortiGate SSL VPN technology, and describes how to configure web-only mode and tunnel-mode SSL VPN access for remote users through the web-based manager.
- *FortiGate PPTP VPN User Guide*

  Explains how to configure a PPTP VPN using the web-based manager.
- *FortiGate Certificate Management User Guide*

  Contains procedures for managing digital certificates including generating certificate requests, installing signed certificates, importing CA root certificates and certificate revocation lists, and backing up and restoring installed certificates and private keys.
- *FortiGate VLANs and VDOMs User Guide*

  Describes how to configure VLANs and VDOMS in both NAT/Route and Transparent mode. Includes detailed examples.

Fortinet Knowledge Center

The knowledge center contains troubleshooting and how-to articles, FAQs, technical notes, and more. Visit the Fortinet Knowledge Center at http://kc.forticare.com.

Comments on Fortinet technical documentation

Please send information about any errors or omissions in this document, or any Fortinet technical documentation, to techdoc@fortinet.com.

Customer service and technical support

Fortinet Technical Support provides services designed to make sure that your Fortinet systems install quickly, configure easily, and operate reliably in your network.

Please visit the Fortinet Technical Support web site at http://support.fortinet.com to learn about the technical support services that Fortinet provides.

Upgrade Notes

Before downloading FortiOS 3.0, it is recommended that you read this chapter to learn about on the new features and/or changes to existing features with the operating system. This chapter describes these changes and features, new to FortiOS 3.0.

We recommend also reviewing the *FortiGate CLI Reference* guide for the new and revised CLI commands as well as the *FortiGate Administration Guide*.

This section includes the following:

Backing up configuration files

You now have the option to backup configuration files with or without encryption. If you back up without encrypting the file, the FortiGate unit saves the file in a clear text format. VPN certificates are saved only when selecting the encrypted setting.

Setup Wizard

The setup wizard is discontinued.

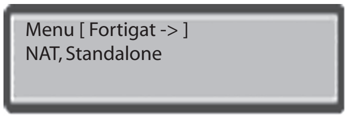
FortiLog name change

The FortiLog logging appliance has been renamed to **FortiAnalyzer** for version 3.0. The name change better reflects the product’s more robust reporting and logging features.

LCD display changes

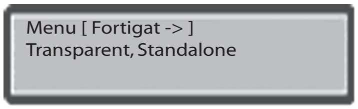
After upgrading to FortiOS 3.0, FortiGate units with an LCD screen will display the following main menus:

Figure 1: LCD main menu settings for NAT/Route mode



Menu [Fortigat ->]
NAT, Standalone

Figure 2: LCD main menu setting for Transparent mode

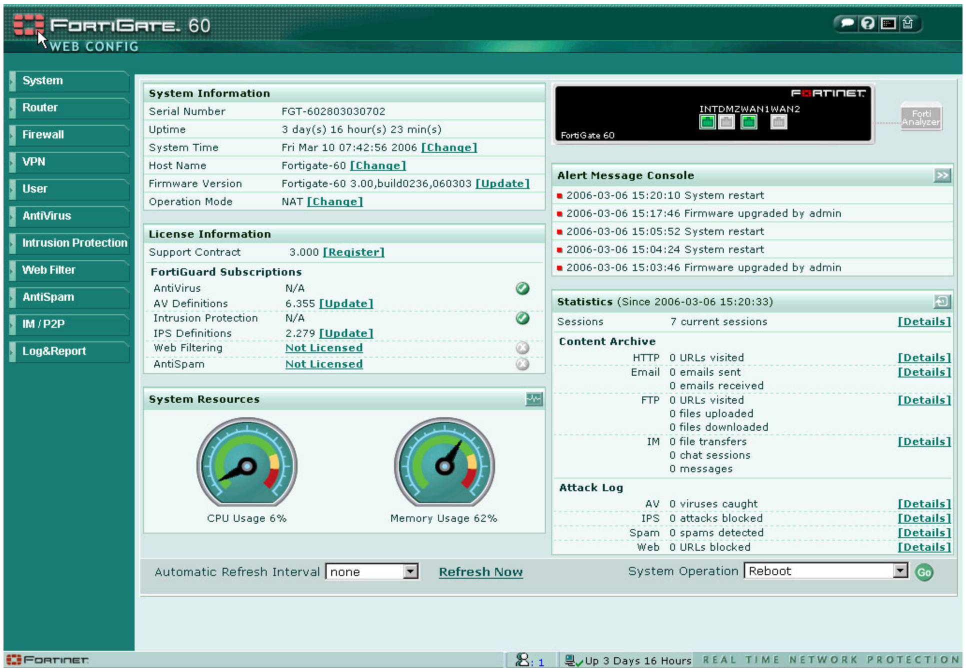


Menu [Fortigat ->]
Transparent, Standalone

Web-based manager changes

The system dashboard in FortiOS 3.0 has been enhanced, with various system information now categorized and additional features added to better monitor your FortiGate unit.

Figure 3: System Dashboard of a FortiGate-60



System Information

Serial Number	FGT-602803030702
Uptime	3 day(s) 16 hour(s) 23 min(s)
System Time	Fri Mar 10 07:42:56 2006 [Change]
Host Name	Fortigate-60 [Change]
Firmware Version	Fortigate-60 3.00,build0236,060303 [Update]
Operation Mode	NAT [Change]

License Information

Support Contract	3.000 [Register]	
FortiGuard Subscriptions		
AntiVirus	N/A	✓
AV Definitions	6.355 [Update]	
Intrusion Protection	N/A	✓
IPS Definitions	2.279 [Update]	
Web Filtering	Not Licensed	☒
AntiSpam	Not Licensed	☒

System Resources

Automatic Refresh Interval none

Alert Message Console

- 2006-03-06 15:20:10 System restart
- 2006-03-06 15:17:46 Firmware upgraded by admin
- 2006-03-06 15:05:52 System restart
- 2006-03-06 15:04:24 System restart
- 2006-03-06 15:03:46 Firmware upgraded by admin

Statistics (Since 2006-03-06 15:20:33)

Sessions	7 current sessions	[Details]
Content Archive		
HTTP	0 URLs visited	[Details]
Email	0 emails sent 0 emails received	[Details]
FTP	0 URLs visited 0 files uploaded 0 files downloaded	[Details]
IM	0 file transfers 0 chat sessions 0 messages	[Details]
Attack Log		
AV	0 viruses caught	[Details]
IPS	0 attacks blocked	[Details]
Spam	0 spams detected	[Details]
Web	0 URLs blocked	[Details]

System Operation Reboot

System Information

Serial Number	The FortiGate device's serial number.
Up Time	The amount in days, hours and minutes the FortiGate device has been running.
System Time	The day, month, and time the FortiGate device has for its specified time zone.
Host Name	The name of the FortiGate device. Select Update to change the host name.

	Firmware Version	The current firmware version. Select Update to install new firmware.
	Operation Mode	The mode the FortiGate device is running in. Select Update to change the operation mode.
System Resources		
	CPU usage	The CPU usage amount in percent.
	Memory usage	The amount of memory used in percent.
	The history of these and other resources is available by selecting the History icon in the top right-hand corner of the System Resources category.	
License Information		
	Support Contract	The expiry date and version of your support contract.
	FortiGuard Subscription	The subscriptions you have for your FortiGate device and displays whether they are current, need updating or when they will expire.
Alert Message Console		Displays system alert messages. These messages display any firmware upgrades or downgrades and if the system restarted. The console also displays an alert message if the antivirus engine is low on memory for a specific time period.
Statistics		Displays detail statistics for the content archive and attack logs.

The FortiGate image in the upper-right-hand corner of the web-based manager, displays the status of the unit's port settings. When you hover your mouse over a port, it displays the port name, IP/Netmask address, link status, speed, including the number of packets sent and received. The port appears gray if it is not connected, and green if the port is connected. The FortiAnalyzer image is gray when the FortiGate unit is not connected to a FortiAnalyzer unit.

Changes to the web-based manager

In FortiOS 3.0, there are several features that have merged with other features. See the "New features and changes" on page 17 for more information.

If you need additional information on these new features, see *FortiGate Administration Guide.*

Command Line Interface changes

The Command Line Interface (CLI) commands have changed and additional commands added. See the *FortiGate CLI Reference* for more information.

Also, some FortiOS 2.80MR11 web-based manager features have been moved to the CLI. See the "New features and changes" on page 17 for information on these changes.

USB support

The USB is supported in FortiOS 3.0. The FortiUSB key (purchased separately) enables you to backup configuration files and restore backed up configuration files. You can even configure the FortiGate unit to automatically install a firmware image and restore configuration settings on a system reboot using the FortiUSB key.

For more information, see the *Install Guide* for your FortiGate unit.

The following FortiGate units support the FortiUSB key:

- FortiGate-60/60M
- FortiWiFi-60
- FortiWiFi-60A/60AM
- FortiGate-100A
- FortiGate-200A
- FortiGate-300A
- FortiGate-400A
- FortiGate-500A
- FortiGate-800/800F
- FortiGate-5001SX
- FortiGate-5001FA2
- FortiGate-5002FB2

Note: The FortiGate unit only supports the FortiUSB key, available from Fortinet.

Other

The following are other issues you should be aware of not included in the above sections or in “New features and changes” on page 17.

- Antivirus scanning, blocking and quarantine is available for instant messaging file transfers with AIM, MSN, Yahoo, and ICQ.
- The Antivirus monitor is configured in the CLI.
- Calendar date is represented in YYYY-MM-DD format.
- If the daylight savings time feature is enabled, you need to manually reset the system clock when daylight savings time ends.
- “Report Bug to Fortinet” link is only available in the CLI.
- FDS Registration Link is accessed by selecting **System > Status > License Information > Support Contract**.
- Internet browsing for IPSec now requires two policies.
- Web Filter/AntiSpam list are now specific to each protection profile. This is only for FortiGate-800 units and above.
- Administration access for a VLAN interface in a virtual domain is unavailable in the web-based manager. Use the `get system interface <VLAN>` command.

- WLAN upgrades are unsuccessfully since during the upgrade process the wireless daemon is turned off to conserve memory.
- Certain IPS group settings are not carried forward. You need to manually configure these settings after upgrading.
- Lists from FortiOS 2.80MR11 cannot be restored in FortiOS 3.0. Make sure to document these lists before upgrading. If you upgrade using the web-based manager, these lists may carry forward. Use both the web-based manager and CLI to verify these lists carried forward if you upgraded using the web-based manager.

See the *Release Notes FortiOS 3.0MR1* for more information.

New features and changes

There are several new features included in FortiOS 3.0, as well as changes to existing features. This chapter outlines the new features as well as the changes.

Before you proceed to upgrade your FortiGate unit, it is recommended you review this document and the following documents to familiarize yourself the new features and changes.

- *FortiGate Administration Guide*
- *FortiGate CLI Reference*

The following topics are included in this section:

- System
- Firewall
- VPN
- User
- Antivirus
- Intrusion Protection (formerly IPS)
- Web Filter
- AntiSpam (formerly Spam Filter)
- IM/P2P (new)
- Log & Report

Note: Configuration of settings in the following menus are unchanged unless otherwise stated.

System

The System menu consists of the following:

- Status
- Network
- Config
- Admin
- Maintenance

Note: The DHCP menu is not included since its unchanged from FortiOS v2.80MR11.

Status

The Status page displays the System Dashboard. The System Dashboard is categorized and five new items have been added:

- CPU, memory usage statistics history
- FortiGuard Subscription-based services and license information
- Image of the FortiGate unit’s port status settings
- Image of a FortiAnalyzer unit and its connectivity status to the FortiGate unit
- An AV/IPS/Content statistics summary table.

The System Dashboard also displays a login monitor that displays how many administrators are logged in. This feature provides administrators (with system configuration write access profiles) to disconnect other admin users, if required. You can even refresh the FortiGate system and shutdown the FortiGate unit from this page. See “Web-based manager changes” on page 12 for more information on the System Dashboard.

Sessions

The Sessions information is now located in **System > Status > Statistics**.

Network

The Network tab appears in the System menu. Modem settings for the FortiGate-60, FortiWiFi-60, and the FortiGate-50A are only available through the CLI. See the *FortiGate CLI Reference* for more information.

The Options tab now has Dead Gateway Detection, previously in **System > Config > Options**.

Config

The tabs for this menu have changed. The Time tab information is now located in **System > Status > System Information > System Time**.

The Options tab is now available in **System > Admin > Settings**. This tab also includes Virtual Domain Configuration, Web Administration Ports, including Web Administration. The Web Administration is now called Language.

HA, SNMP v1/v2c and Replacement Messages tabs are still in the Config menu.

Operation Mode is available from this menu, and can also be found in **System > System Information > Operation Mode**.

The FortiManager tab has moved to the Admin menu.

Admin

The Admin menu includes two new tabs along with the previous tabs, the Administrators and Access Profile.

In the Administrators tab, you can configure an access profile while configuring a new administrator.

The FortiManager tab is now located in the Admin menu. The Settings tab is also new to the Admin menu.

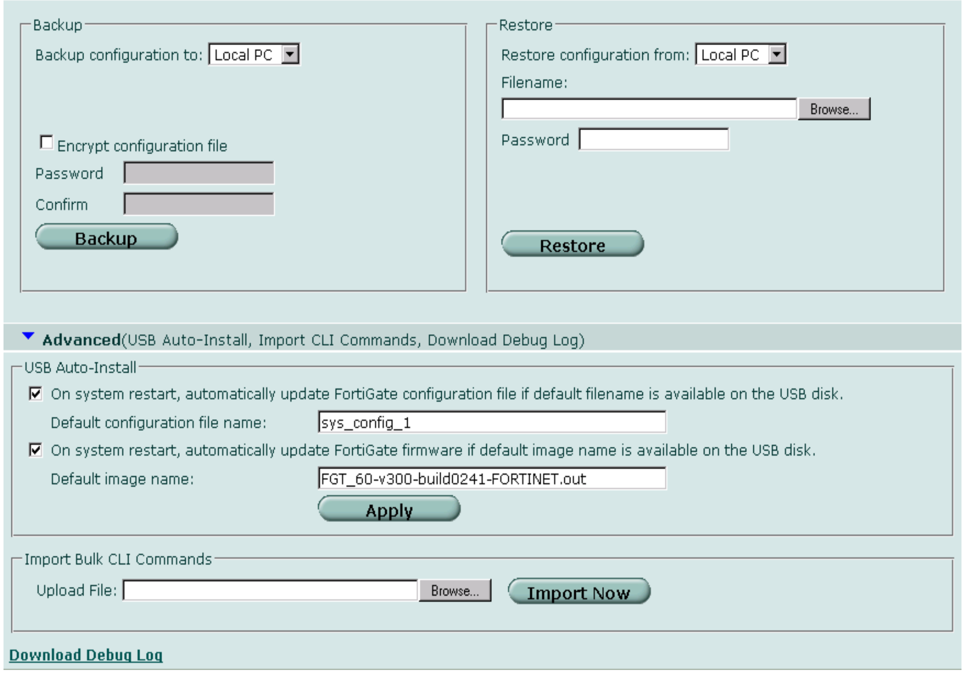
Maintenance

The Maintenance menu now has only two tabs, Backup and Restore and FortiGuard Center.

The Backup and Restore tab has several new options available for backing up and restoring configuration files. From this tab you can backup, or restore, a configuration file and select to encrypt the configuration file. You also select your Local PC or FortiUSB key (if supported by the FortiGate unit) to backup or restore your configuration files. The Backup and Restore tab also features an Advanced option, enabling you to use the FortiUSB key for automatically installing a configuration file or image file if the system restarts. You can also import CLI commands.

Also, there is a Download Debug log option. You can download an encrypted debug log to a file and then send it to Fortinet Technical Support to help diagnose problems with your FortiGate unit.

Figure 4: Backup and Restore page



Backup

Backup configuration to: Local PC

□ Encrypt configuration file

Password

Confirm

Backup

Restore

Restore configuration from: Local PC

Filename: Browse...

Password

Restore

▼ **Advanced**(USB Auto-Install, Import CLI Commands, Download Debug Log)

USB Auto-Install

☑ On system restart, automatically update FortiGate configuration file if default filename is available on the USB disk.

Default configuration file name: sys_config_1

☑ On system restart, automatically update FortiGate firmware if default image name is available on the USB disk.

Default image name: FGT_60-v300-build0241-FORTINET.out

Apply

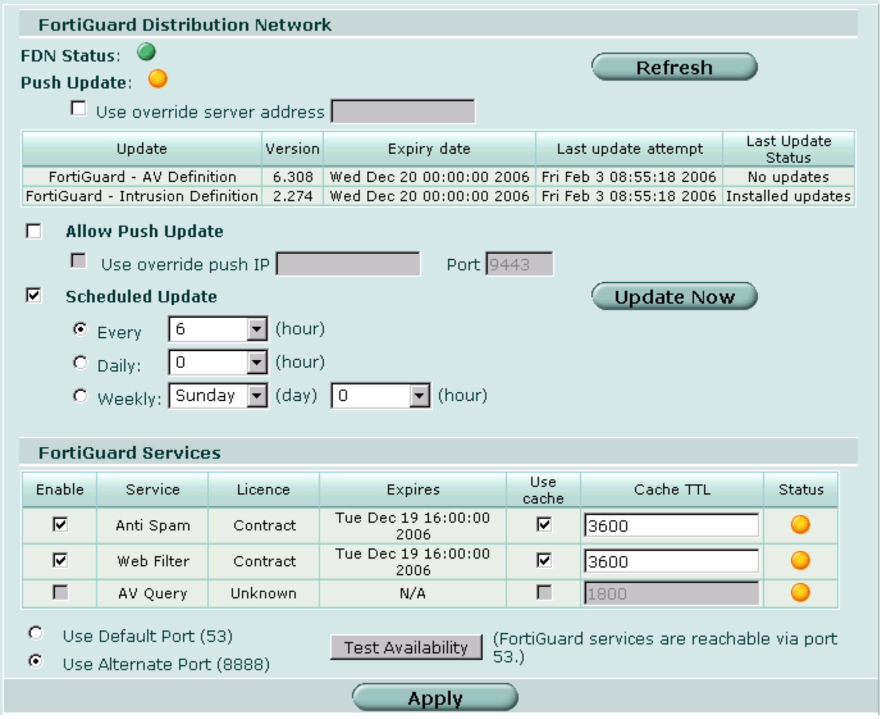
Import Bulk CLI Commands

Upload File: Browse... Import Now

Download Debug Log

The FortiGuard Center, previously the Update Center, displays several options for enabling the FortiGate unit to connect to the Fortinet Distribution Network (FDN), and for updating antivirus and attack definitions. You can also test the availability of FortiGuard services from this page.

Figure 5: FortiGuard Center page



FortiGuard Distribution Network

FDN Status: ●

Push Update: ●

☐ Use override server address

Update	Version	Expiry date	Last update attempt	Last Update Status
FortiGuard - AV Definition	6.308	Wed Dec 20 00:00:00 2006	Fri Feb 3 08:55:18 2006	No updates
FortiGuard - Intrusion Definition	2.274	Wed Dec 20 00:00:00 2006	Fri Feb 3 08:55:18 2006	Installed updates

☐ Allow Push Update

☐ Use override push IP Port 9443

☑ Scheduled Update

● Every 6 (hour)

○ Daily: 0 (hour)

○ Weekly: Sunday (day) 0 (hour)

FortiGuard Services

Enable	Service	Licence	Expires	Use cache	Cache TTL	Status
☑	Anti Spam	Contract	Tue Dec 19 16:00:00 2006	☑	3600	●
☑	Web Filter	Contract	Tue Dec 19 16:00:00 2006	☑	3600	●
☐	AV Query	Unknown	N/A	☐	1800	●

○ Use Default Port (53)

● Use Alternate Port (8888)

(FortiGuard services are reachable via port 53.)

The following tabs are no longer in the Maintenance menu:

- Support tab is no longer available.
- Shutdown is now located on **System > Status > System Operation**.

Virtual Domain

This menu is now an option in **System > Admin > Settings**. When you enable this option, you must log back into the web-based manager to configure VDOM settings. Both the web-based manager and CLI change as follows to reflect VDOM:

- Global and per VDOM configurations are separated
- only admin administrator accounts can view or configure global options
- admin administrator accounts can configure all VDOM configurations
- admin administrator accounts can connect through any interface in the root VDOM
- admin administrator accounts can connect through any interface that belongs to a VDOM that a regular administration account has been assigned
- a regular administration account can only configure the VDOM it is assigned to and access the FortiGate interface belonging to that VDOM
- a regular administration account can create a VLAN subinterface in its own VDOM on a physical interface in its own VDOM

- an administration account with access profile that provides read and write access to
- only the admin administrator account can configure a VDOM unless you create and assign a regular administrator to that VDOM

Router

The Router menu consists of the following menus:

- Static
- Dynamic
- Monitor

Static

The Static menu has two tabs, Policy Route and Static Route. The Policy Route tab was previously a menu in the Router menu.

Dynamic

The Dynamic menu is new and includes four tabs to configure Routing Information Protocol (RIP), Open Shortest Path First (OSPF), Border Gateway Protocol (BGP), and Multicast protocols.

Dynamic routing protocols enable the FortiGate unit to automatically share information about routes with neighboring routers, including learning about routers and networks advertised by neighboring routers.

- RIP protocol is a distance-vector routing protocol for small networks, or similar networks.
- OSPF is slightly different, and is a link-state routing protocol, most often used in large networks to share networking information among the routers in the same autonomous system.
- BGP is an Internet routing protocol, typically used by ISPs to exchange routing information between different ISP networks. For example, a BGP enables the sharing of network paths between the ISP network and an autonomous system that uses RIP and/or OSPF to route packets within the autonomous system.
- Multicast enables the FortiGate unit to operate as a Protocol Independent Multicast (PIM) version 2 router in the root virtual domain. The PIM routers throughout the network ensure only one copy of the packet is forwarded until it reaches an end-point destination and at this destination copies of the packet are made only when required to deliver the information to multicast client applications requesting traffic destined for the multicast address.

Note: The following are now in the CLI:

- Distribution list
- Offset list
- Pre-fix list
- Route-Map
- Key-chain
- Access list

Monitor

The Routing Monitor tab displays the entries in the FortiGate routing table. You can apply a filter to display certain routes to search for specific routing protocols.

Firewall

The Firewall menu consists of the following menus:

- Policy
- Address
- Service
- Virtual IP
- Protection Profiles

Policy

The Policy menu is very similar to the menu in FortiOS 2.80MR11. However, there is no advanced option when you are creating a new policy. Also, there is authentication and traffic shaping checkboxes along with two additional options, Protection Profile and Log Allowed Traffic.

When you select Traffic Shaping, you can then select guaranteed bandwidth, maximum bandwidth, and the traffic priority.

Address

The Address menu now has the option to select the type of address you are creating. The type of address can be Subnet/IP Range or Fully Qualified Domain Name (FQDN).

Note: The FQDN should be used with caution, since it presents security risks.

Service

The Custom tab has a new look in the Service menu. From the Custom tab, you can add as many TCP/UDP protocols that you need to the custom service.

Virtual IP

The Virtual IP has additional options and the IP Pool menu is now a tab included in this menu.

Protection Profiles

The Protection Profiles menu has two additional options for you to select from, the IM/P2P and Logging option.

VPN

The VPN menu contains the following menus:

- IPSec
- SSL
- Certificates

The VPN menu has several significant changes for FortiOS 3.0. Configuration of VPNs has also significantly changed. It is recommended you read the *Release Notes FortiOS 3.0MR1* to review known issues and changes for configuring VPNs.

Note: VPN settings may need to be reconfigured after you upgrade to FortiOS 3.0. Also, VPN IPSec Phase 2 settings source and destination ports are reset to zero during the upgrade.

Note: The CLI command `auto-negotiate` replaces the Ping generator feature. The `auto-negotiate` is disabled by default and is available for both IPSec tunnels in the IPSec Phase 2 configuration for both IPSec tunnels.

IPSec

The IPSec menu has changed to reflect the way you configure VPNs. Phase 1 and Phase 2 tabs are merged with the new AutoKey (IKE) tab. The Ping Generator tab is now available in the CLI. See the *FortiGate CLI Reference* for more information.

SSL

The SSL menu is new for FortiOS 3.0. There are two tabs, Config and Monitor where you can configure SSL VPNs and monitor

The Secure Socket Layer uses a cryptographic system that uses two keys to encrypt data, a public key and private key.

If you require SSL version 2 encryption for compatibility with older browsers, you can enable this protocol through the CLI, in the VPN chapter. See the *FortiGate CLI Reference* for more information on SSL. Also, you can enable the use of digital certificates for authenticating remote clients.

Certificates

The Certificates menu has a new tab, Certificate Revocation List (CRL). The FortiGate unit uses CRLs to ensure certificates belonging to CAs and remote clients are valid.

From the CRL tab you can also import these types of certificates. It is important to periodically retrieve certificate revocation lists from CA web sites to ensure clients that have revoked certificates cannot establish a connection with the FortiGate unit.

Note: After downloading a CRL from a CA web site, save the CRL on a computer that has management access to the FortiGate unit.

User

The User menu consists of the following menus:

- Local
- Radius
- LDAP
- Windows AD
- User Group

Local

The Local menu is unchanged.

Radius

The Radius menu is unchanged.

LDAP

The LDAP menu is unchanged. However, it now has the Common Name Identifier, Distinguished Name, and Server Port fields on the LDAP page. The Server Secret field is now located in the CLI, under Radius in the User chapter. See the *FortiGate CLI Reference* for more information.

Windows AD

The Windows AD menu, new for FortiOS 3.0, enables you to configure your FortiGate unit on a Windows Active Directory (AD) network so it can transparently authenticate the user without asking for their username and password.

From the Windows AD menu, you can create a new Windows AD server and delete, edit or refresh the server.

Note: The Fortinet Server Authentication Extensions (FSAE) is included on your Fortinet Documentation and tools CD, or from the Technical Support website at https:\\support.fortinet.com.

User Group

The User Group menu is unchanged. However, you can now choose the type of user group from the following:

- Firewall
- Active Directory
- SSL VPN

You can also select the FortiGuard Web Filtering Override option on the User Group page to enable your FortiGate unit to allow FortiGuard web filtering overrides.

Antivirus

The Antivirus menu is now located below the User menu. It consists of the following menus:

- File Pattern
- Quarantine
- Config

File Pattern

The File Pattern menu has changed. The columns on the File Pattern page are now Pattern, Action and Enable. When you select Create New, you can select the pattern, type of action to take (either Block or Allow) and whether the new file pattern should be enabled or disabled.

Quarantine

The Quarantine menu is new to the Antivirus menu. It contains two tabs, Quarantined Files and Config. The Quarantined Files tab displays the information of each file, displaying why the file was blocked. You can also filter the files by file name, date, service, status, and status description.

The Config tab displays a list of current viruses the FortiGate unit has blocked and you can configure file and email size limits, including grayware blocking.

Note: You need to be connected to the FortiAnalyzer unit to configure file and email size limits, including grayware blocking.

Config

The Config menu includes the Virus List and Grayware tabs. The Config tab is now located in the CLI under Antivirus Service. See the *FortiGate CLI Reference* for more information.

Intrusion Protection (formerly IPS)

The Intrusion Protection menu consists of the following menus:

- Signature
- Anomaly

Note: Make sure to document all FortiOS 2.80 IPS group settings before upgrading to FortiOS 3.0, since certain IPS group settings are not carried forward and must be configured manually. See the *Release Notes FortiOS 3.0MR1* for more information.

Signature

The Signature menu is unchanged. However, you can now view the severity level of pre-defined signatures and custom signatures. Also, you can reset the pre-defined signatures to their default settings if you changed them.

When creating new custom signatures on the Custom page, you can specify the severity level for the custom signature.

Anomaly

The Anomaly menu detects and identifies network traffic that attempts to take advantage of known exploits.

When you are creating a new anomaly, you can now specify the severity, and instead of selecting Logging, you now select Packet Log. The field called Parameters is no longer available.

Protocol Decoder

The Protocol Decoder menu, new for FortiOS 3.0 displays protocol anomalies for logging purposes. You can enable or disable logging for a protocol anomaly, and configure the IPS action in response to detecting an anomaly. If you require to revert back to default settings, you can select the Reset icon.

You can use the CLI to configure session control based on source and destination address. The protocol anomaly list is updated when the firmware image is upgraded.

Web Filter

The Web Filter menu consists of the following menus. It is now located under Intrusion Protection.

- Content Block
- URL Filter
- FortiGuard-Web Filter

Note: The lists you configured in FortiOS 2.80 may carry forward to FortiOS 3.0 if you upgrade using the web-based manager. Make sure to document these lists for reference to verify after the upgrade is successful. See the *Release Notes for FortiOS 3.0MR1* for more information.

Content Block

The Content Block menu has a new tab called Web Content Exempt.

URL Filter

The URL Filter menu allows or blocks access to specific URLs. You can also add patterns or expressions to allow or block URLs. The URL Filter menu has Web URL Block tab and Web Pattern Block tab.

In FortiOS v2.80MR11, URL Filter used to be URL Block. Web Filter is now merged with URL Filter.

FortiGuard-Web Filter

The FortiGuard-Web Filter menu, formerly under **Web Filter > Category Block > Configuration**, is now its own menu in the Web Filter menu.

The FortiGuard-Web is a managed web filtering solution provided by Fortinet, sorting hundreds of millions of web pages into a wide range of categories for users to allow, block, or monitor.

The FortiGuard-Web Filter menu contains the Override tab, Local Categories tab and Local Ratings tab. On FortiGate units with a hard disk, you can create reports from the Reports tab.

The Override tab provides administrators with flexibility and control when blocking web pages. Administrators can configure override rules that allow users to access blocked web pages, if required. Administrators can also create user-defined categories to allow users to block groups of URLs on a per-profile basis.

From the Local Ratings tab you can configure local ratings to specify whether the local rating is used in conjunction with the FortiGate rating or is used as an override. The Local Categories tab allows you to specify user-defined categories and then specify the URLs that belong to the category.

AntiSpam (formerly Spam Filter)

The Antispam menu consists of the following menus:

- Banned word
- Black/White list

You can configure additional features for FortiGate-800 units and above. In the Banned word list you can:

- create new antispam banned word list
- view antispam banned word catalog

You can also configure the following for the FortiGate-800 and above in the Black/White list:

- add multiple email address lists
- create new antispam email address list
- create new antispam IP address list
- view antispam IP address list catalog

The previous options available from the web-based manager in FortiOS v2.80MR11, are now available in the CLI. See the *FortiGate CLI Reference* for more information. This includes FortiGuard AntiSpam, IP Address, DNSBL and ORDBL, MIME Headers, and Email Address.

If the MIME header check is enabled for POP3, IMAP or SMTP, and any change is made to the Protection Profile, such as IP address check, banned word check or logging oversized files (enabled through the web-based manager), the MIME header check is disabled.

Also, the “clear” action for banned words in an email is now available in the CLI to support upgrade. Since the “clear” action is no longer a valid spam action in FortiOS 3.0, avoid using it when configuring banned words.

Note: The Black/White lists are not separate. You may need to re-enable MIME Headers when you upgrade to FortiOS 3.0.

Banned word

The Banned word menu still controls spam by blocking email messages containing specific words or patterns. The Action column on the Banned Word page is now Score, and is reflected when configuring a new banned word.

Score is a numerical weighting applied to banned word. If the score is greater than the spamwordthreshold value set in the protection profile, the page is processed according to whether the spam action command for the mail traffic type (for example `smtp3-spamaction`) is set to pass or tag in the protection profile. The score for the banned word is counted once even if the word appears multiple times in the web page.

Black/White list

The Black/White list menu provides a way to filter incoming email if enabled in the protection profile. The FortiGate unit uses both an IP address list and email list for filtering purposes.

The FortiGate unit compares the IP address of the message's sender to the IP address in sequence when doing an IP address list check. If the FortiGate unit finds a match, the action associated with the IP address is taken. If there is no match, then the message passes to the next enabled spam filter.

Email lists work the same way.

IM/P2P (new)

The IM/P2P menu consists of the following menus:

- Statistics
- User

The IM/P2P menu is new for FortiOS 3.0. Since instant messaging and peer to peer (P2P) networks have grown, FortiOS 3.0 now includes a separate menu for these new technologies. You can control the amount of bandwidth allocated for P2P.

There are extended features with the IM/P2P menu, available in the CLI. You can use `config imp2p old-version` command to enable older versions of IM protocols. These older versions of IM protocols are able to bypass file blocking because the message types are not recognized. This command provides the option to disable these older IM protocol versions.

The supported protocols are:

- MSN 6.0 and above
- ICQ 4.0 and above
- AIM 5.0 and above
- Yahoo 6.0 and above

Note: The FortiGate unit is unable to block Skype uses. Also, if the audio blocking feature is enabled, instant messaging clients are still able to send/receive webcam/video traffic.

Statistics

The Statistics menu provides administrators with a view of instant messaging and point to point statistics to gain insight into how these protocols are being used within the network.

The Overview tab provides detail statistics for all IM/P2P protocols. The Protocol tab displays statistics for current users, blocked users and users since last reset.

User

The User menu displays which instant messenger users are connected. Network administrators can analyze the list and decide which users to allow or block.

The Config tab enables administrators to configure what to do with unknown users.

Log & Report

The Log and Report menu has a new menu, Report. Log & Report consists of the following menus:

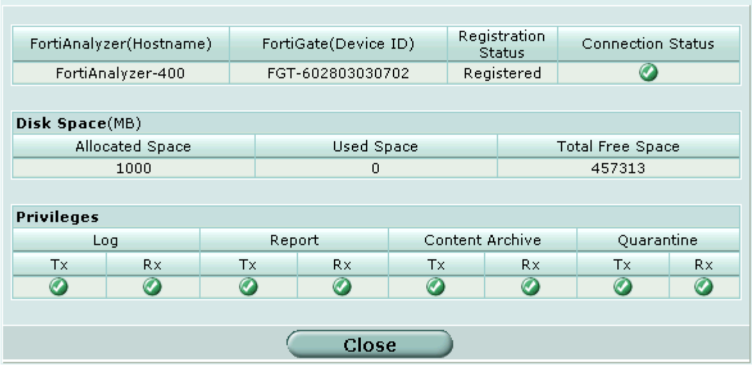
- Log Config
- Log Access
- Report

Log Config

The Log Config menu has a new tab, Event Log. The Event Log tab enables you to choose the events you want logged. This menu also includes the Alert E-mail tab. The Alert E-mail tab is the same as in FortiOS v2.80MR11, providing immediate notification of issues occurring on the FortiGate unit, such as system failures or network attacks.

In the Log Setting tab, you can test the connectivity between the FortiGate unit and the FortiAnalyzer unit to check connection status.

Figure 6: Test connectivity feature in Log and Report



FortiAnalyzer(Hostname)	FortiGate(Device ID)	Registration Status	Connection Status
FortiAnalyzer-400	FGT-602803030702	Registered	✓

Disk Space(MB)

Allocated Space	Used Space	Total Free Space
1000	0	457313

Privileges

Log		Report		Content Archive		Quarantine	
Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx
✓	✓	✓	✓	✓	✓	✓	✓

Also, instead of configuring the connection between the two devices, you can enable a new feature called FortiDiscovery to automatically discover and connect to a FortiAnalyzer unit. The FortiDiscovery feature uses HELLO packets to locate the FortiAnalyzer unit(s) that are on the network within the same subnet.

The web trends option and traffic filtering are now available in the CLI. See the *FortiGate CLI Reference* for more information.

Logging options for various protocols and traffic is now in the Protection Profiles menu.

Note: Log filter is now included in **Firewall > Protection Profile > Logging**. You can also enable this feature in the CLI. Also, Traffic Filter is now available in the CLI. See the *FortiGate CLI Reference* for more information.

Log Access

The Log Access menu has two tabs. The Memory tab displays log event types that are logged to memory. The FortiAnalyzer tab displays log types that are logged to the FortiAnalyzer unit.

An additional tab for Disk appears on FortiGate units with a hard disk. Use the pull-down menu to select a different log type.

Report

The Report menu, new to the Log and Report menu, provides you with access to a full range of different reports from the FortiAnalyzer unit if connected.

You can choose the Basic Traffic report or access any type of FortiAnalyzer report to display logs. The Basic Traffic report uses log information stored in the FortiGate unit’s memory and displays the information in two types of bar graphs on the Report Access page.

You can choose from over a thousand of FortiAnalyzer reports to display logs. Also, you can customize a default report for your FortiGate unit.

You can also select what you want included in your report from Newsgroups to VoIP.

HA

There are significant changes, including new features, for high availability in FortiOS 3.0. The most significant change for HA is virtual clustering, where you can configure HA for individual virtual domains. The virtual clustering can handle two FortiGate units per virtual cluster.

The *FortiGate Administration Guide* (System Config chapter, HA section), *FortiGate CLI Reference* (system chapter, ha section), and the *FortiGate online help* provides additional information on changes to existing features and new features in FortiOS 3.0.

In the System menu, HA is now a tab in **System > Config > HA**. You can configure HA settings for your FortiGate unit from this tab. However, Unit Priority setting is now Device Priority and Override Master is now enabled by default.

Note: The *FortiGate High Availability (HA) Guide* will be available soon.

Upgrading the HA cluster for FortiOS 3.0

The following procedure will help you upgrade a FortiOS 2.80 HA cluster to FortiOS 3.0.

You can use either the web-based manager or the `execute restore image` CLI command and a TFTP server to upgrade the cluster.

To upgrade the cluster

1 Backup the configurations of the primary unit. See "Backing up your configuration" on page 33.

2 Install the firmware image on the primary unit.

This may take a few minutes since the primary unit will upgrade the subordinate units as well. The FortiGate units in the cluster will reboot once or twice during the upgrade.

Note: The primary/subordinate roles may change during the upgrade, if HA override is not enabled before upgrading.

SNMP MIBs and traps changes

In FortiOS 3.0 the trap file is combined into the MIB file - there is only one MIB file to download and install to your SNMP management system.

SNMP traps and variables that used hyphens (for example xxx-yyy) have dropped the hyphen and capitalized the second term (xxxYyy).

The v3.0 MIB file also has more in-depth descriptions, and supports models. To see these changes, contact Fortinet technical support to obtain the MIB file.

In-depth SNMP trap changes

The following table displays trap name changes, including additional trap names for FortiOS 3.0.

FortiOS v3.0 trap name / status	FortiOS v2.8 trap name / status
`fnFMTrapIfChange`	New
`fnFMTrapConfChange`	New
No longer available	`fnTrapHaStateChange`
No longer available	`fnTrapIdsPortScan`
No longer available	`fnTrapImTableFull`

In-depth MIB file name changes

The following table displays trap name changes, including additional trap names for FortiOS 3.0.

Location	FortiOS v3.0 trap name / status	FortiOS v2.8 trap name / status
System	`fnSysDiskCapacity`	New
	`fnSysDiskUsage`	New

	fnSysMemCapacity	New
HA	fnHaLBSchedule	fnHaSchedule
	fnHaGroupID	fnHaGroupID
	fnHaPriority	No longer available
	fnHaOverride	No longer available
	fnHaAutoSync	No longer available
Options	fnOptAuthTimeout	New
	fnOptionLanguage	New
	fnOptLcdProtection	New
Management	fnManSysSerial	New
	fnManIfName	New
	fnManIfIp	New
	fnManIfMask	New
Administrator Accounts	fnAdminTable	
	perm	No longer available

Upgrading to FortiOS 3.0

Before you begin upgrading to FortiOS 3.0, it is recommended that you first review this chapter as well as the release notes so you can be fully aware of these new features and changes.

This chapter includes the following sections:

- Backing up your configuration
- Upgrading your FortiGate unit
- Verifying the upgrade

Note: You can now configure the FortiGate unit to perform NAT functions in Transparent mode if you network configuration requires this particular network scenario. See the *Release Notes FortiOS 3.0MR1* for more information.

Backing up your configuration

Fortinet recommends that you back up all configuration settings from your FortiGate unit(s) before upgrading to FortiOS 3.0.

Use the following procedures to backup your configuration file(s) for FortiOS v2.80MR11 in either the web-based manager or the CLI.

Note: Always backup your configuration before upgrading to a current firmware version, or when resetting to factory defaults.

Backing up your configuration using the web-based manager

Use the following procedure to backup your current configuration in the web-based manager.

To backup your configuration file using the web-based manager

1 Go to **System > Maintenance > Backup & Restore**.

2 For All Configuration Files, select the Backup icon.

3 Select OK.

4 Save the file.

Note: You can enter a password to encrypt the configuration file when backing up.

Backing up your configuration using the CLI

Use the following procedure to backup up your current configuration in the CLI.

To backup your configuration file using the CLI

Backup the configuration file. Enter:

```
execute backup allconfig <filename> <address_ip>
```

This may take a few minutes.

After successfully backing up your configuration file(s), either from the CLI or the web-based manager, proceed with the upgrade to FortiOS 3.0.

Upgrading your FortiGate unit

You can upgrade to FortiOS 3.0 using either the web-based manager or CLI. Use the following procedures to upgrade your existing firmware version to FortiOS 3.0.

If upgrading to FortiOS 3.0 is unsuccessful, go to "Reverting to FortiOS v2.80MR11" on page 37 to downgrade to FortiOS 2.80MR11. If your upgrade is successful and your FortiGate unit has a hard-drive, you can use the Boot alternate firmware option located on the Backup and Restore page. This option enables you to have two firmware images, such as FortiOS 2.80MR11 and FortiOS 3.0, for downgrading/upgrading purposes. Use the Fortinet Knowlege Center article 2.80MR11 to 3.0MR1 upgrade/downgrade/dual-boot to configure a dual-boot/configuration for your FortiGate unit.

You may need to reconfigure some configuration settings in FortiOS 3.0. See the *Release Notes FortiOS 3.0MR1* for more information.

Note: Make sure you have upgraded to FortiOS v2.80MR11 before upgrading to FortiOS 3.0.

Upgrading to FortiOS 3.0

This section describes the procedures for upgrading to FortiOS 3.0 using either the web-based manager or CLI.

Upgrading using the web-based manager

You can use the web-based manager to upgrade to FortiOS 3.0. Use the following procedure for upgrading to FortiOS 3.0.

Note: Before proceeding, make sure you back up your configuration. Also, it is recommended you use the CLI to upgrade to FortiOS 3.0. However, a TFTP upgrade reverts all current firewall configurations to factory default settings. Use the web-based manager if you want to carry forward certain FortiOS 2.80MR11 settings.

To upgrade to FortiOS 3.0 using the web-based manager

1. Copy the firmware image file to your management computer.
2. Log into the web-based manager.
3. Go to **System > Status > Unit Information**.

4 Under Unit Information, select Update.

5 Type the path and filename of the firmware image file, or select Browse and locate the file.

6 Select OK.

The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, restarts, and displays the FortiGate login. This process may take a few minutes.

Once the upgrade is successfully installed:

- Ping to your FortiGate unit to verify there is still a connection.
- Clear the browser's cache and log into the web-based manager.

After logging back into the web-based manager, you should save your configuration settings that carried forward. Some settings may have carried forward from FortiOS 2.80MR11, while others may not have such as certain IPS group settings. Go to **System > Maintenance > Backup and Restore** to save the configuration settings that carried forward.

Note: After upgrading to FortiOS 3.0, perform an "Update Now" to retrieve the latest AV/NIDS signatures from the FortiGuard Distribution Network (FDN) as the signatures included in the firmware may be older than those currently available on the FDN.

Upgrading using the CLI

Use the following procedures to upgrade to FortiOS 3.0 in the CLI.

To upgrade to FortiOS 3.0 using the CLI

1 Make sure the TFTP server is running.

2 Copy the new firmware image file to the root directory of the TFTP server.

3 Log into the CLI.

4 Make sure the FortiGate unit can connect to the TFTP server

You can use the following command to ping the computer running the TFTP server. For example, if the IP address of the TFTP server is 192.168.1.168:

```
execute ping 192.168.1.168
```

5 Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

```
execute restore image <name_str> <tftp_ip4>
```

When `<name_str>` is the name of the firmware image file and `<tftp_ip>` is the IP address of the TFTP server. For example, if the firmware image file name is `image.out` and the IP address of the TFTP server er is 192.168.1.168, enter:

```
execute restore image.out 192.168.1.168
```

The FortiGate unit responds with a message similar to the following:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

6 Type `y`.

The FortiGate unit uploads the firmware image file, upgrades to the new firmware version, and restarts. This process takes a few minutes.

7 Reconnect to the CLI.

8 To confirm the firmware image is successfully installed, enter:

```
get system status
```

9 Update antivirus and attack definitions (see the *FortiGate Administration Guide*), or from the CLI, enter:

```
execute update-now
```

Verifying the upgrade

After logging back into the web-based manager, you will notice your FortiOS v2.80MR11 configuration settings have been carried forward. For example, if you go to **System > Network > Options** you can see your DNS settings carried forward from your FortiOS v2.80MR11 configuration settings.

Even though your configuration settings have carried forward, you should verify these settings. Verifying your settings also gives you an opportunity to familiarize yourself with the new features and changes in FortiOS 3.0.

You can verify your configuration settings by:

- going through each menu and tab in the web-based manager
- using the `show` shell command in the CLI

Also, check to make sure the administrative access settings you configured for your FortiGate unit were carried forward.

Reverting to FortiOS v2.80MR11

You may need to revert to a pervious firmware version if the upgrade did not install successfully. The following sections will help you to backup your current FortiOS 3.0 configuration, downgrade to FortiOS v2.80MR11, and restore your FortiOS v2.80MR11 configuration.

The following topics are included in this section:

- Backing up your FortiOS 3.0 configuration
- Downgrading to FortiOS v2.80MR11 using web-based manager
- Downgrading to FortiOS v2.80MR11 using the CLI

Backing up your FortiOS 3.0 configuration

If you have configured additional settings in FortiOS 3.0, it is recommended that you back up your FortiOS 3.0 configuration before downgrading to FortiOS v2.80MR11. This ensures you have a current configuration file for FortiOS 3.0 if you decide to upgrade.

Use the following procedure to backup your configuration onto your PC.

To backup your configuration to your PC

1 Go to **System > Maintenance > Backup & Restore**.

2 Select Local PC from Backup Configuration to list.

If you want to encrypt your configuration file to save VPN certificates, select the Encrypt configuration file checkbox and enter a password, then enter it again to confirm.

3 Select Apply.

Backing up to a FortiUSB key

You can also backup your FortiOS 3.0 configuration to the FortiUSB key. Before proceeding, ensure the FortiUSB key is inserted in the FortiGate unit USB port. Use the following procedure to backup your configuration onto your FortiUSB.

Note: Always make sure the FortiGate unit is shutdown and powered off when you insert the FortiUSB key into the key into the FortiGate unit’s USB port.

To backup your configuration using the FortiUSB key

1 Go to **System > Maintenance > Backup & Restore**.

2 Select USB Disk from Backup Configuration to list.

If you want to encrypt your configuration file to save VPN certificates, select the Encrypt configuration file checkbox and enter a password, then enter it again to confirm.

3 Select Apply.

Downgrading to FortiOS v2.80MR11 using web-based manager

When you downgrade to FortiOS v2.80MR11, only the following settings are retained:

- Operation mode
- Interface IP/Management IP
- Route static table
- DNS settings
- VDOM parameters/settings
- Admin user account
- Session helpers
- System accprofiles

Use the following procedure to downgrade to FortiOS v2.80MR11 in the web-based manager. If you have created additional settings in FortiOS 3.0, make sure you back up your configuration before downgrading. See for more “Backing up your FortiOS 3.0 configuration” on page 37 information.

To downgrade using the web-based manager

1. Go to **System > Status > Firmware Version**.
2. Select Update.
3. Type the location of the firmware version or select Browse.
4. Select OK.

   The following message appears:

   ```
   The new image does not support CC mode. Do you want to
   continue to upgrade?
   ```
5. Select OK.

   The following message appears:

   ```
   This version will downgrade the current firmware version.
   Are you sure you want to continue?
   ```
6. Select OK.

   The FortiGate unit uploads the firmware image file, reverts to the old firmware version, resets the configuration, restarts, and displays the FortiGate login. This process takes a few minutes.
7. Log into the web-based manager.

   Go to **System > Unit Information** to verify the Firmware Version has changed to FortiOS v2.80MR11.

Verifying the downgrade

After successfully downgrading to FortiOS 2.80MR11, verify your connections and settings. If you are unable to connect to the web-based manager, make sure your administration access settings and internal network IP address are correct. The downgrade may change your configuration settings to default settings.

Downgrading to FortiOS v2.80MR11 using the CLI

Use the following procedure to downgrade to FortiOS v2.80MR11 in the CLI. If you have created additional settings in FortiOS 3.0, make sure you back up your configuration before downgrading. See "Backing up your FortiOS 3.0 configuration" on page 37 for more information.

To downgrade using the CLI

1 Make sure the TFTP server is running.

2 Copy the firmware image file to the root directory of the TFTP server.

3 Log into the FortiGate CLI.

4 Make sure the FortiGate unit can connect to the TFTP server.

You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server's IP address is 192.168.1.168:

```
execute ping 192.168.1.168
```

5 Enter the following command to copy the firmware image from the TFTP server to the FortiGate unit:

```
execute restore image tftp <name_str> <tftp_ipv4>
```

Where `<name_str>` is the name of the firmware image file and `<tftp_ipv4>` is the IP address of the TFTP server. For example, if the firmware image file name is image.out and the IP address of the TFTP server er is 192.168.1.168, enter:

```
execute restore image tftp image.out
192.168.1.168
```

The FortiGate unit responds with the message:

```
This operation will replace the current firmware version! Do
you want to continue? (y/n)
```

6 Type `y`.

The FortiGate unit uploads the firmware image file. After the file uploads, a message similar to the following is displayed:

```
Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```

7 Type `y`.

The FortiGate unit reverts to the old firmware version, resets the configuration to factory defaults, and restarts. This process takes a few minutes.

After the FortiGate unit uploads the firmware, you will need to reconfigure your IP address since the FortiGate unit reverts to default settings, including its default IP address. See your install guide for configuring IP addresses.

8 Reconnect to the CLI.

9 To confirm the new firmware image has been loaded, enter:

```
get system status
```

See "Restoring your configuration" on page 40 to restore you FortiOS v2.80MR11 configuration settings.

Restoring your configuration

Your configuration settings may not have carried over after you have downgraded to FortiOS v2.80MR11. You can restore your configuration settings for FortiOS v2.80MR11 with the configuration file(s) you saved before upgrading to FortiOS 3.0.

Restoring your configuration settings using the web-based manager

You can restore the FortiOS v2.80MR11 configuration settings using the web-based manager. Use the following procedure to restore these settings.

To restore configuration settings using the web-based manager

1. Log into the web-based manager.
2. Go to **System > Maintenance > Backup & Restore**.
3. Select the Restore icon for All Configuration Files.
4. If required, enter your password for the configuration file.
5. Type the location of the file or select Browse to locate the file.
6. Select OK.

   The FortiGate unit restores the configuration settings for FortiOS v2.80MR11. This may take a few minutes since the FortiGate unit will reboot.

   To verify the configuration settings are restored, log into the web-based manager and go through the menus and tabs and verify the settings are restored.

Restoring your configuration settings using the CLI

You can restore the FortiOS v2.80MR11 configuration settings using the CLI. Use the following procedure to restore these settings.

To restore configuration settings using the CLI

1. Make sure the TFTP server is running.
2. Copy the backup configuration file to the root directory of the TFTP server.
3. Log into the TFTP server.
4. Make sure the FortiGate unit can connect to the TFTP server.

   You can use the following command to ping the computer running the TFTP server. For example, if the TFTP server’s IP address is 192.168.1.168:

   ```
   execute ping 192.168.1.168
   ```

5 Enter the following command to copy the backup configuration file to restore the file on the FortiGate unit:

```
execute restore allconfig <name_str> <tftp_ipv4> <passwrd>
```

Where `<name_str>` is the name of the backup configuration file and `<tftp_ipv4>` is the IP address of the TFTP server and `<passwrd>` is the password you entered when you backup your configuration settings. For example, if the backup configuration file is `confall` and the IP address of the TFTP server is 192.168.1.168 and the password is `ghrffdt123`:

```
execute restore allconfig confall 192.168.1.168 ghrffdt123
```

The FortiGate unit responds with the message:

```
This operation will overwrite the current settings and the
system will reboot!
Do you want to continue? (y/n)
```

6 Type `y`.

The FortiGate unit uploads the backup configuration file. After the file uploads, a message, similar to the following, is displayed:

```
Getting file confall from tftp server 192.168.1.168
##
Restoring files...
All done. Rebooting...
```

This may take a few minutes.

Use the `show` shell command to verify your settings are restored, or log into the web-based manager.

See “Restoring your configuration” on page 40 to restore you FortiOS v2.80MR11 configuration settings.

Index

www.fortinet.com

FORTINET™

www.fortinet.com